UNITED STATES DISTRICT COURT

for the
Eastern District of Wisconsin

In the Matter of the Search of:

Information associated with the Facebook user IDs 100012891004557, 100025143570455, 1529468944, and 100009337719641 that is stored at premises owned, maintained, controlled, or operated by Facebook, a company headquartered in Menlo Park, California.

Case No. 19-852M(NJ)

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property:

See Attachment A

located in the Eastern District of Wisconsin, there is now concealed:

See Attachment B

The basis for the search under Fed. R. Crim P. 41(c) is:

- ☒ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to violations of: Title 18, United States Code, Sections 2251(a), 2252(a)(4)(B) and 2423(c).

The application is based on these facts: See attached affidavit.

☐ Delayed notice of _____ days (give exact ending date if more than 30 days:_____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Special Agent Kevin C. Wrona, HSI
Printed Name and Title

Sworn to before me and signed in my presence:

Date: May 8, 2019

Judge's signature

City and State: Milwaukee, Wisconsin

Hon. Nancy Joseph, U.S. Magistrate Judge
Printed Name and Title

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, Kevin C. Wrona, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent with the U.S. Department of Homeland Security, U.S. Immigration and Customs Enforcement, Homeland Security Investigations ("HSI"), and have been so employed since June 2010. I am currently assigned to the HSI Office of the Resident Agent in Charge in Milwaukee, Wisconsin. My duties include investigating criminal violations relating to child exploitation and child pornography including violations of advertising, producing, distributing, receiving, and possessing child pornography, in violation of Title 18, United States Code, Sections 2251 and 2252 and travel with the intent to engage in illicit sexual conduct, in violation of Title 18, United States Code, Section 2423(b). I have received training in the investigation of child pornography and child exploitation offenses and have observed and reviewed numerous examples of electronically-stored child pornography.

2. I make this affidavit in support of an application for a search warrant for information associated with certain accounts that are stored, owned, maintained, controlled, or operated by Facebook, a social network provider located at 1601 Willow Road, Menlo Park, California 94025. The information to be searched consists of three (3) accounts (hereinafter, the Subject Accounts) and is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to

require Facebook to disclose to the government copies of the information (including the content of communications) further described in Attachment B.

3. The purpose of this application is to seize evidence more particularly described in Attachment B, of violations of 18 U.S.C. § 2423(c), which make it a crime to travel in foreign commerce or reside, either temporarily or permanently, in a foreign country, and engage in any illicit sexual conduct with another person who has not attained the age of eighteen; 18 U.S.C. § 2251(a), which makes it a crime to employ, use, persuade, induce, entice, or coerce any minor to engage in any sexually explicit conduct for the purpose of producing any visual depiction of such conduct or for the purpose of transmitting a live visual depiction of such conduct, and 18 U.S.C. § 2252(a)(4)(B), which makes it a crime to knowingly possesses, or knowingly accesses with intent to view, one or more books, magazines, periodicals, films, video tapes, or other matter which contain any visual depiction that has been mailed, or has been shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, or which was produced using materials which have been mailed or so shipped or transported, by any means including by computer, if the producing of such a visual depiction involves the use of a minor engaging in sexually explicit conduct.

4. The statements contained in this Affidavit are based my experience and background as a Special Agent with HSI, and by information provided by other law enforcement agents. Some information in this affidavit also comes from information received from the issuance of administrative summonses. Because this affidavit is being

submitted for the limited purpose of securing a search warrant, I have not included every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that evidence of violations of Title 18, United States Code, Sections 2423, 2251, and 2252 is located in the accounts described in Attachment A.

DEFINITIONS

5. The following definitions applies to this Affidavit and Attachment B to this Affidavit:

a. "Chat" refers to any kind of communication over the Internet that offers a real-time transmission of text messages from sender to receiver. Chat messages are generally short in order to enable other participants to respond quickly and in a format that resembles an oral conversation. This feature distinguishes chatting from other text-based online communications such as Internet forums and email.

b. "Child pornography," as used herein, is defined in 18 U.S.C. § 2256 (any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct).

c. "Cloud Storage" refers to saving data to an off-site storage system maintained by a third party. Instead of exclusively storing information to the

computer's hard drive or other local storage devices, the user saves it to a remote database (and or both). The Internet provides the connection between the computer and the database. There are several cloud-based storage options available to consumers (Dropbox, Google Drive, Box, Copy, Amazon, One Drive), with the majority of them offering gigabytes of storage free of charge.

d. "Internet Service Providers" (ISPs), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment. ISPs can offer a range of options in providing access to the Internet including telephone-based dial-up, broadband based access via digital subscriber line (DSL) or cable television, dedicated circuits, or satellite-based subscription. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth, which the connection supports. Many ISPs assign each subscriber an account name – a user name or screen name, an "e-mail address," an e-mail mailbox, and a personal password selected by the subscriber. By using a computer equipped with a modem, the subscriber can establish communication with an ISP over a telephone line, through a cable system or via satellite, and can access the Internet by using his or her account name and personal password.

e. "ISP Records" are records maintained by ISPs pertaining to their subscribers (regardless of whether those subscribers are individuals or entities). These records may include account application information, subscriber and billing

information, account access information (often in the form of log files), e-mail communications, information concerning content uploaded and/or stored on or via the ISP's servers, and other information, which may be stored both in computer data format and in written or printed record format. ISPs reserve and/or maintain computer disk storage space on their computer system for their subscribers' use. This service by ISPs allows for both temporary and long-term storage of electronic communications and many other types of electronic data and files.

f. "Internet Protocol address" or "IP address" refers to a unique number used by a computer to access the Internet. IP addresses can be dynamic, meaning that the Internet Service Provider (ISP) assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be static, if an ISP assigns a user's computer a particular IP address which is used each time the computer accesses the Internet. IP addresses are also used by computer servers, including web servers, to communicate with other computers.

g. "Minor" means any person under the age of eighteen years. *See* 18 U.S.C. § 2256(1).

h. The terms "records," "documents," and "materials," include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or

magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, Bernoulli drives, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

i. "Sexually explicit conduct" means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person. *See* 18 U.S.C. § 2256(2).

BACKGROUND ON PEOPLE WITH AN INTEREST IN CHILD PORNOGRAPHY AND ONLINE CHILD EXPLOITATION

6. Based on my training and experience, as well as the training and experience of other law enforcement personnel with whom I have spoken, I have learned the following:

a. Individuals who possess, transport, receive, and/or distribute child pornography often collect sexually explicit materials, which may consist of photographs, videos, computer graphics or other images, as well as literature describing sexually explicit activity involving children. Many of these individuals also collect child erotica, which consist of items that may not rise to the level of child pornography, but which nonetheless serve a sexual purpose involving children.

b. Individuals who possess, transport, receive, and/or distribute child pornography often seek out like-minded individuals, either in person or on the Internet, to share information and trade depictions of child pornography and child erotica. The different Internet-based vehicles used by such individuals to communicate with each other include, but are not limited to, peer-to-peer file sharing and other similar interfaces.

c. Individuals who possess, transport, receive, and/or distribute child pornography often collect, read, copy, or maintain names, addresses (including e-mail addresses), phone numbers, or lists of individuals who have advertised or otherwise made known in publications and on the Internet that they have similar sexual interests. These contacts are maintained as a means of personal referral, exchange, or commercial profit. These names may be maintained in computer storage devices, or in remote storage accounts.

d. Individuals who possess, transport, receive, and/or distribute child pornography rarely, if ever, dispose of their sexually explicit materials and may go to great lengths to conceal and protect their collections of illicit materials from discovery, theft, and damage. One way to store child pornography without keeping the material on a specific device is to use cloud-based file storage services such as Google Drive, which can be accessed through an internet connection from any computer.

BACKGROUND ON NATIONAL CENTER FOR MISSING AND EXPLOITED CHILDREN

7. Based on my training and experience, and publicly available information, I know that the National Center for Missing and Exploited Children (NCMEC) is a nonprofit organization in Alexandria, Virginia, that works with law enforcement on issues related to missing and sexually exploited children. One of the services provided and administered by NCMEC is its CyberTipline, which serves as the national clearinghouse for leads regarding sexual exploitation crimes against children.

8. In addition to reports from the general public, reports are made by U.S. electronic communication service (ECS) providers and remote computing services (RCS), which are required by 18 U.S.C. § 2258A to report "apparent child pornography" to NCMEC via the CyberTipline if they become aware of the content on their servers. Specially trained analysts, who examine and evaluate the reported content, review leads, add related information that may be useful to law enforcement, use publicly available search tools to determine the geographic location of the apparent criminal act, and ultimately provide all of the gathered information to the appropriate law enforcement agency for review and possible investigation.

9. The CyberTipline receives reports, known as CyberTips, about the possession, production and distribution of child pornography; online enticement of children for sexual acts; child prostitution; sex tourism involving children; child sexual molestation; unsolicited obscene material sent to a child; misleading domain names; and misleading words or digital images on the Internet.

10. The CyberTip reports will vary in detail depending on the nature of the report, and which entity submits it. The reports can include information (1) relating to the identity of any individual who appears to have violated federal law by committing or attempting to commit the criminal conduct described above; (2) historical information on when or how a customer or subscriber of an ECS or RCS uploaded, transmitted, or received apparent child pornography; (3) geographical information on the involved individual or website, which may include the IP Address or verified billing address or geographic identifying information, including area code or zip code; (4) any images of apparent child pornography; and (5) the complete communication containing any image of apparent child pornography. See 18 U.S.C. § 2258A(b).

PROBABLE CAUSE

Initial Information Received from the National Center for Missing and Exploited Children (NCMEC)

11. On June 20, 2018, I was provided a CyberTip from NCMEC regarding Facebook usernames engaging in sexually explicit conduct. According to CyberTip (CT) 35013606, accounts with user names Don Stevenson and Donald White were used to entice apparent minors to engage in sexual activity. The CT was reported to NCMEC directly from Facebook, and included Facebook user names, Facebook user ID numbers, e-mail addresses and internet protocol (IP) addresses used to access the Facebook accounts. According to the CyberTip, these two accounts, along with an account with

the user name Don Stenson, were linked by machine cookie,[1] indicating the Facebook accounts were being logged into using the same electronic device.

12. These three (3) accounts, along with one other, are the Subject Accounts. The Facebook user ID for user name Don Stevenson is 100012891004557. The Facebook user ID for the user name Donald White is 100025143570455. The Facebook user ID for the user name Don Stenson is 1529468944. I am also seeking evidence for Facebook account Don Chonmanee, with Facebook user ID: 100009337719641. As described below, possible underage victims who were identified and interviewed cited the Facebook user account Don Chonmanee as another account used by Donald Stenson to communicate with them. Also, I identified Donald Stenson as the person likely using the Don Stevenson and Donald White accounts. The HSI liaison to NCMEC conducted research into various combinations of the first and last names, and dates of birth for the White/Stevenson/STENSON accounts, as provided by Facebook in the cybertip, and identified an individual named: Donald Arthur STENSON, DOB: XX/XX/1956, with an associated address of: XXXX S. 101st., St., Milwaukee, WI 53227. As explained below, subscriber information to an internet protocol (IP) address used by White/Stevenson comes back to the above address. While I do not have evidence the Don Stenson account (1529468944) was used to communicate with minors or to arrange sexual encounters with minors, I believe information obtainable by the warrant could provide

---

[1] Facebook provided associated accounts via "cookie" technology. Cookies are a small text file created by a website that is stored in the user's computer either temporarily for that session only or permanently on the hard disk. Cookies provide a way for the website to recognize you and keep track of your preferences.

geolocation information about his travel, and possibly provide information about where and when he met the victims. Additionally, he may use his real account to document his travel.

13. I have reviewed the messages, parts of which are shown below. Based on my training and experience, it appears the Facebook user for the Don Stevenson and Donald White accounts enticed multiple, allegedly underage, Facebook users located in the Philippines to engage in sexual chats. Additionally, this Facebook user, using multiple Facebook accounts, indicated he planned to travel to the Philippines and expressed an interest in engaging in sexual activity with minor females.

14. Excerpts of the conversations between Facebook user Don Stevenson (Facebook ID: 100012891004557), and MVAL (Facebook ID: 100014305757229), as provided by CT 35013606, are as follows:

Sender	Date	Time	Message
Don Stevenson	09/22/2017	2:41:17 am PDT	I look forward to seeing you because I think I will be excited to see you on video chat
Don Stevenson	09/22/2017	2:41:33 am PDT	And if u wanna see my excitement, I can share that too.. he he <3
MVAL	09/22/2017	02:41:49 am PDT	me too hehehe
Don Stevenson	09/22/2017	02:42:52 am PDT	ahahaha.. my excitement might include an erection.. ha ha ha.. sorry joke
MVAL	09/22/2017	02:43:17 am PDT	hahaha
Don Stevenson	09/22/2017	02:44:00 am PDT	Aira... ur so sweet.. thx for chat today
MVAL	09/22/2017	02:44:29 am PDT	welcome sir :)
Don Stevenson	09/22/2017	02:46:37 am PDT	If ur here, I give you a big hug

MVAL	09/22/2017	02:46:55 am PDT	Heheehe
Don Stevenson	09/22/2017	02:47:21 am PDT	and your first kiss.. ha ha ha.. joking again
MVAL	09/22/2017	02:47:33 am PDT	Hmmmmn
Don Stevenson	09/22/2017	02:48:36 am PDT	On your cheek
Don Stevenson	09/22/2017	02:50:13 am PDT	And boobs..
MVAL	09/22/2017	02:50:33 am PDT	hehe

15. The following is an excerpt from Facebook communication between Facebook users Donald White (Facebook ID: 100025143570455) and MVSE (Facebook ID: 100014674219418), as provided by CT 35013606:

Sender	Date	Time	Message
Donald White	04/17/2018	10:48 pm PDT	Beautiful AF
MVSE	04/17/2018	10:49 pm PDT	If i come too meet to U
MVSE	04/17/2018	10:49 pm PDT	U give me money
Donald White	04/17/2018	10:50 pm PDT	Of course. I will pay for transportation and bonding
MVSE	04/17/2018	10:50 pm PDT	Yeahh i like it
Donald White	04/17/2018	10:51 pm PDT	My friend asks if you are a virgin
MVSE	04/17/2018	10:52 pm PDT	Yes I'm virgin
Donald White	04/17/2018	10:52 pm PDT	We respect that
MVSE	04/17/2018	10:52 pm PDT	Hah
Donald White	04/17/2018	10:53 pm PDT	But we can cure that if you wish
Donald White	04/17/2018	11:00	Can you show boobs on video call?

		pm PDT	

16. The following is an excerpt from a Facebook communication between Facebook user Donald White (Facebook ID: 100025143570455) and MVMH (Facebook ID: 100023948806018), as provided by CT 35013606:

Sender	Date	Time	Message
Donald White	05/02/2018	04:14 am PDT	You will start High School grade 7 in June?
MVMH	05/02/2018	04:15 am PDT	yes
Donald White	05/14/2018	08:12 am PDT	I miss you
MVMH	05/14/2018	08:12 am PDT	ok
Donald White	05/14/2018	08:12 am PDT	We can take a shower?
MVMH	05/14/2018	08:13 am PDT	yes
Donald White	05/14/2018	08:16 am PDT	Thank you in advance
MVMH	05/14/2018	08:16 am PDT	ok
Donald White	05/14/2018	08:28 am PDT	We can kiss? muah muah muah
MVMH	05/14/2018	06:51 pm PDT	ok
Donald White	05/14/2018	09:56 pm PDT	I love you
MVMH	05/21/2018	11:06 pm PDT	How old ar you
Donald White	05/21/2018	11:07 pm PDT	50 … and you?
Donald White	05/21/2018	11:10 pm PDT	How old are you?
MVMH	05/21/2018	11:56 pm PDT	13
Donald White	05/22/2018	12:10 am PDT	Oh. So young. I will be kind and respectful

17. On September 14, 2018, I issued a Department of Homeland Security (DHS) summons to Charter Communication, requesting subscriber information for IP addresses: 172.220.77.181, 2605:a000:bce0:2c00:b17b:8b26:1673:cfbf, and 2605:a000:bcc0:b100:ad38:bd92:2cc3:fd86, which were the IP addresses associated with the Donald White Facebook account that engaged in chats with allegedly underage females.

18. On September 14, 2018, Charter responded to the summons indicating that IP addresses: 2605:a000:bce0:2c00:b17b:8b26:1673:cfbf and 2605:a000:bcc0:b100:ad38:bd92:2cc3:fd86 were registered to John Burgdorff, XXXX S. 101st St., West Allis, WI 53227, XXXX@wi.rr.com, XXX-XXX-1463 and XXX-XXX-9792. It also indicated that IP address: 172.220.77.181 is registered to: Ellen Jessen, XXXX Turquoise Ln., Madison, WI 53714, XXX-XXX-7046, and XXXX@charter.net.

19. Open source research conducted on both John Burgdorff and XXXX S. 101st St., West Allis showed both Donald STENSON and John Burgdorff as residents. A check of the Wisconsin Department of Transportation database found that Burgdorff has the address listed as his address of record, and the West Allis property search database shows Burgdorff as the owner of the house.

20. Open source research conducted on both Ellen Jessen and XXXX Turquoise Ln., Madison showed Ellen Jessen as a resident, but did not show Donald STENSON was as well. A check of the Wisconsin Department of Transportation database found that Jessen has the address listed as her address of record. The WIDOT

record also indicated that Jessen was previously Ellen Stenson in June 1992, The Dane County Assessor's Office indicated that house is owned by "Springer/Jessen Trust".

21. Research conducted by NCMEC on various combinations of the user account names, and the dates of birth provided for them identified an individual: Donald A. Stenson, DOB: XX/XX/1956, with an associated address of XXXX S. 101st., St., Milwaukee, WI 53227.

22. HSI Attaché Manila was able to confirm that STENSON traveled to the Philippines multiple times since February 2007, most recently between January 6, 2019 and January 22, 2019. HSI Attaché Manila was working with Philippine authorities to identify and confirm the ages of the three possible minor female victims cited in CT 35013606.

23. On March 21, 2019, HSI Attaché Manila contacted HSI Milwaukee. During March 18, 2019 through March 21, 2019, HSI Manila, with the assistance of the HSI Manila Transnational Criminal Investigative Unit (TCIU), located and identified four (4) victims who are Philippine nationals that were victims of child sexual exploitation by STENSON. One of the victims is an adult and was sexually abused as a minor, and the other three (3) victims are 13, 15, and 16 years of age. The four victims positively identified STENSON as the person who molested them by encircling the picture of STENSON through a photographic line-up.

24. During an interview by Philippine authorities, one of the four minor females stated that she met STENSON in 2017, when she was 12 years old. She stated that in October 2017, she and other underage minor victims met STENSON at his hotel

room and proceeded to masturbate him while he (STENSON) fondled their breasts. She stated that after they finished, STENSON paid each of the females some money. She stated that she would masturbate STENSON once a week over the course of three weeks. She further stated that on top of the money, STENSON would give her gifts, to include food, clothing, laptops, cellphones and tablet. Additionally, she stated that STENSON used the Facebook account Don Chonmanee.

Investigation into Donald Stenson

25. As part of this investigation, I queried a DHS database for Donald Stenson and saw it showed frequent international travel. Since June 2010, STENSON has made frequent trips into the United States, generally staying several weeks, before departing again. STENSON last departed the United States via San Francisco International Airport on July 17, 2018, and traveled to Tokyo, Japan.

26. On June 19, 2001, STENSON was referred to U.S. Immigration secondary at Los Angeles International Airport for further inspection. There, inspectors noted that STENSON was traveling with a minor child, who is a citizen of Thailand, and will be in the United States for six (6) weeks.

27. On June 10, 2015, Customs and Border Protection (CBP) Officers escorted STENSON to the baggage control inspection area for inspection. During inspection, officers found that STENSON was arriving from Thailand, and will be visiting a friend who lives at XXXX S. 101st St., West Allis, WI. STENSON further stated that he has been living in Thailand for 19 years, and that he works for the company "taxezy.com", which prepares income tax forms for J-1 students. Officers found that STENSON would be

staying 5 weeks in the United States. During inspection, officers found a "couple of questionable underage female pics" and recommended additional inspection for possible involvement in child pornography/child sex tourism.

28. A check of the Wisconsin Department of Transportation database found that Donald Arthur STENSON, DOB: XX/XX/1956, has a valid and current Wisconsin driver's license, with XXXX S. 101st St., West Allis, WI 53227 as his address of record.

FACEBOOK

29. Facebook owns and operates a free-access social networking website of the same name that can be accessed at http://www.facebook.com. Facebook allows its users to establish accounts with Facebook, and users can then use their accounts to share written news, photographs, videos, and other information with other Facebook users, and sometimes with the general public.

30. Facebook asks users to provide basic contact and personal identifying information to Facebook, either during the registration process or thereafter. This information may include the user's full name, birth date, gender, contact e-mail addresses, Facebook passwords, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers. Facebook also assigns a user identification number to each account.

31. Facebook users may join one or more groups or networks to connect and interact with other users who are members of the same group or network. Facebook assigns a group identification number to each group. A Facebook user can also connect directly with individual Facebook users by sending each user a "Friend Request." If the

recipient of a "Friend Request" accepts the request, then the two users will become "Friends" for purposes of Facebook and can exchange communications or view information about each other. Each Facebook user's account includes a list of that user's "Friends" and a "News Feed," which highlights information about the user's "Friends," such as profile changes, upcoming events, and birthdays.

32. Facebook users can select different levels of privacy for the communications and information associated with their Facebook accounts. By adjusting these privacy settings, a Facebook user can make information available only to himself or herself, to particular Facebook users, or to anyone with access to the Internet, including people who are not Facebook users. A Facebook user can also create "lists" of Facebook friends to facilitate the application of these privacy settings. Facebook accounts also include other account settings that users can adjust to control, for example, the types of notifications they receive from Facebook.

33. Facebook users can create profiles that include photographs, lists of personal interests, and other information. Facebook users can also post "status" updates about their whereabouts and actions, as well as links to videos, photographs, articles, and other items available elsewhere on the Internet. Facebook users can also post information about upcoming "events," such as social occasions, by listing the event's time, location, host, and guest list. In addition, Facebook users can "check in" to particular locations or add their geographic locations to their Facebook posts, thereby revealing their geographic locations at particular dates and times. A particular user's profile page also includes a "Wall," which is a space where the user and his or her

"Friends" can post messages, attachments, and links that will typically be visible to anyone who can view the user's profile.

34. Facebook allows users to upload photos and videos, which may include any metadata such as location that the user transmitted when s/he uploaded the photo or video. It also provides users the ability to "tag" (i.e., label) other Facebook users in a photo or video. When a user is tagged in a photo or video, he or she receives a notification of the tag and a link to see the photo or video. For Facebook's purposes, the photos and videos associated with a user's account will include all photos and videos uploaded by that user that have not been deleted, as well as all photos and videos uploaded by any user that have that user tagged in them.

35. Facebook users can exchange private messages on Facebook with other users. Those messages are stored by Facebook unless deleted by the user. Facebook users can also post comments on the Facebook profiles of other users or on their own profiles; such comments are typically associated with a specific posting or item on the profile. In addition, Facebook has a chat feature that allows users to send and receive instant messages through Facebook Messenger. These chat communications are stored in the chat history for the account. Facebook also has Video and Voice Calling features, and although Facebook does not record the calls themselves, it does keep records of the date of each call.

36. If a Facebook user does not want to interact with another user on Facebook, the first user can "block" the second user from seeing his or her account.

37. Facebook has a "like" feature that allows users to give positive feedback or connect to particular pages. Facebook users can "like" Facebook posts or updates, as well as webpages or content on third party (*i.e.*, non-Facebook) websites. Facebook users can also become "fans" of particular Facebook pages.

38. Facebook has a search function that enables its users to search Facebook for keywords, usernames, or pages, among other things.

39. Each Facebook account has an activity log, which is a list of the user's posts and other Facebook activities from the inception of the account to the present. The activity log includes stories and photos that the user has been tagged in, as well as connections made through the account, such as "liking" a Facebook page or adding someone as a friend. The activity log is visible to the user but cannot be viewed by people who visit the user's Facebook page.

40. Facebook Notes is a blogging feature available to Facebook users, and it enables users to write and post notes or personal web logs ("blogs"), or to import their blogs from other services, such as Xanga, LiveJournal, and Blogger.

41. The Facebook Gifts feature allows users to send virtual "gifts" to their friends that appear as icons on the recipient's profile page. Gifts cost money to purchase, and a personalized message can be attached to each gift. Facebook users can also send each other "pokes," which are free and simply result in a notification to the recipient that he or she has been "poked" by the sender.

42. Facebook also has a Marketplace feature, which allows users to post free classified ads. Users can post items for sale, housing, jobs, and other items on the Marketplace

43. In addition to the applications described above, Facebook also provides its users with access to thousands of other applications ("apps") on the Facebook platform. When a Facebook user accesses or uses one of these applications, an update about the user's access or use of that application may appear on the user's profile page.

44. Facebook uses the term "Neoprint" to describe an expanded view of a given user profile. The "Neoprint" for a given user can include the following information from the user's profile: profile contact information; News Feed information; status updates; links to videos, photographs, articles, and other items; Notes; Wall postings; friend lists, including the friends' Facebook user identification numbers; groups and networks of which the user is a member, including the groups' Facebook group identification numbers; future and past event postings; rejected "Friend" requests; comments; gifts; pokes; tags; and information about the user's access and use of Facebook applications.

45. Facebook also retains Internet Protocol ("IP") logs for a given user ID or IP address. These logs may contain information about the actions taken by the user ID or IP address on Facebook, including information about the type of action, the date and time of the action, and the user ID and IP address associated with the action. For example, if a user views a Facebook profile, that user's IP log would reflect the fact that

the user viewed the profile, and would show when and from what IP address the user did so.

46. Social networking providers like Facebook typically retain additional information about their users' accounts, such as information about the length of service (including start date), the types of service utilized, and the means and source of any payments associated with the service (including any credit card or bank account number). In some cases, Facebook users may communicate directly with Facebook about issues relating to their accounts, such as technical problems, billing inquiries, or complaints from other users. Social networking providers like Facebook typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications.

47. As explained herein, information stored in connection with a Facebook account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, a Facebook user's IP log, stored electronic communications, and other data retained by Facebook, can indicate who has used or controlled the Facebook account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, profile contact information, private messaging logs, status updates, and tagged photos (and the data associated with the foregoing, such as date and time) may

be evidence of who used or controlled the Facebook account at a relevant time. Further, Facebook account activity can show how and when the account was accessed or used. For example, as described herein, Facebook logs the Internet Protocol (IP) addresses from which users access their accounts along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the account access and use relating to the crime under investigation. Such information allows investigators to understand the geographic and chronological context of Facebook access, use, and events relating to the crime under investigation. Additionally, Facebook builds geo-location into some of its services. Geo-location allows, for example, users to "tag" their location in posts and Facebook "friends" to locate each other. This geographic and timeline information may tend to either inculpate or exculpate the Facebook account owner. Last, Facebook account activity may provide relevant insight into the Facebook account owner's state of mind as it relates to the offense under investigation. For example, information on the Facebook account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

48. Therefore, the computers of Facebook are likely to contain all the material described above, including stored electronic communications and information concerning subscribers and their use of Facebook, such as account access information, transaction information, and other account information.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

49. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Facebook to disclose to the government copies of the records and other information (including the content of communications).

50. Based on the forgoing, I request that the Court issue the proposed search warrant.

51. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that – has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

52. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

53. I request that the Court order Facebook not to notify any person (including the subscribers or customers of the account listed in Attachment A) of the existence of the requested warrant before November 8, 2019, or until further order of the Court. Facebook is a provider of an electronic communication service, as defined in 18 U.S.C. § 2510(15), and/or a remote computer service, as defined in 18 U.S.C. § 2711(2). Pursuant to 18 U.S.C. § 2703, I seek a warrant requiring Facebook to disclose records and information in connection with a criminal investigation. This Court has authority under 18 U.S.C. § 2705(b) to issue "an order commanding a provider of electronic communications service or remote computing service to whom a warrant …

is directed, for such period as the court deems appropriate, not to notify any other person of the existence of the warrant … ." *Id.*

54. Here, such an order is appropriate because the requested warrant relates to an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation, and its disclosure may alert the targets to the ongoing investigation. Accordingly, there is reason to believe that notification of the existence of the requested warrant will seriously jeopardize the investigation, by giving the target an opportunity to destroy or tamper with evidence, or otherwise seriously jeopardize an investigation. *See* 18 U.S.C. § 2705(b). Donald STENSON is not aware of the investigation into him. If he were to learn the government is investigating him, he could destroy additional evidence of his crimes that may exist and be revealed during the search of his Facebook accounts.

55. Based on the forgoing, I request that the Court issue the proposed search warrant. Because the warrant will be served on Facebook who will then compile the requested records at a time convenient to it, there exists reasonable cause to permit the execution of the requested warrant at any time in the day or night.

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with the Facebook user IDs 100012891004557, 100025143570455, 1529468944, and 100009337719641 that is stored at premises owned, maintained, controlled, or operated by Facebook, a company headquartered in Menlo Park, California.

ATTACHMENT B

Information to be disclosed by Facebook

To the extent that the information described in Attachment A is within the possession, custody, or control of Facebook, including any messages, records, files, logs, or information that have been deleted but are still available to Facebook, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(£), Facebook is required to disclose the following information to the government for each user ID listed in Attachment A:

(a) All contact and personal identifying information, including full name, user identification number, birth date, gender, contact e-mail addresses, Facebook passwords, Facebook security questions and answers, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers.

(b) All activity logs for the account and all other documents showing the user's posts and other Facebook activities;

(c) All photos uploaded by that user ID and all photos uploaded by any user that have that user tagged in them;

(d) All profile information; News Feed information; status updates; links to videos, photographs, articles, and other

items; Notes; Wall postings; friend lists, including the friends' Facebook user identification numbers; groups and networks of which the user is a member, including the groups' Facebook group identification numbers; future and past event postings; rejected "Friend" requests; comments; gifts; pokes; tags; and information about the user's access and use of Facebook applications;

(e) All other records of communications and messages made or received by the user, including all private messages, chat history, video calling history, and pending "Friend" requests; including the date and time of the communication, the method of communication, and the source and destination of the communication (such as source and destination email addresses, IP addresses, and telephone numbers);

(f) Evidence indicating how and when the Facebook account was accessed or used, to determine the chronological and geographic context of account access, use, and events relating to the crime under investigation and to the Facebook account owner;

(g) Evidence indicating the Facebook account owner's state of mind as it relates to the crime under investigation;

(h) All "check ins" and other location information;

(i) All IP logs, including all records of the IP addresses that logged into the account;

(j) All records of the account's usage of the "Like" feature, including all Facebook posts and all non-Facebook webpages and content that the user has "liked";

(k) All information about the Facebook pages that the account is or was a"fan" of;

(l) All past and present lists of friends created by the account;

(m) All records of Facebook searches performed by the account;

(n) All information about the user's access and use of Facebook Marketplace;

(o) Records of any Facebook accounts that are linked to the Account by machine cookies (meaning all Facebook user IDs that logged into Facebook by the same machine as the Account)The types of service utilized by the user;

(p) The length of service (including start date) and the means and source of any payments associated with the service (including any credit card or bank account number);

(q) All privacy settings and other account settings, including privacy settings for individual Facebook posts and activities,

and all records showing which Facebook users have been blocked by the account;

(r) All records pertaining to communications between Facebook and any person regarding the user or the user's Facebook account, including contacts with support services and records of actions taken; and

(s) Records relating to who created, used, or communicated with the user ID, including records about their identities and whereabouts.